## FULL CONTENTS

[Claim(s)]

[Claim 1] [ the server equipment which accesses the storage which has two or more storage areas to which access restriction was given individually, and this storage, and the backup unit of a removable media method / with predetermined means of communications ] It is the backup management method of the data in storage in the storage system by which network connection is carried out. [ with the key which gave the data of storage area A peculiar to storage area A ] on the occasion of backup of the data of certain storage area A of said storage areas The enciphered encryption data is stored in the predetermined removable media set in said backup unit through said communication network. The encryption data which sets the removable-media-of-relevance-in-said backup unit when restoring the data of storage area A, and is stored in this is transmitted to said storage through said communication network. It is characterized by decrypting by said key to which this was given by storage area A, and storing in storage area A.

[Claim 2] It is the backup management method of the data in storage in a storage system according to claim 1. Said predetermined means of communications is SAN, and said storage area is offered by one set or two or more sets of hard disk units. Encipher by the key which gave the data of a certain hard disk unit A of said hard disk units peculiar to that hard disk unit, and Storage and File Management Sub-Division of this encryption data is carried out to said hard disk unit other than a hard disk unit A. Said encryption data is stored in the predetermined removable media set in said backup unit through said SAN on the occasion of backup of the data of a hard disk unit A. The removable media of relevance is set in said backup unit when restoring the data of a hard disk unit A. It is characterized by decrypting by said key to which the encryption data stored in this was transmitted to said storage through said SAN, and this was given by the hard disk unit A, and making it store in a hard disk unit A.

[Claim 3] It is the backup management method of the data in storage in a storage system according to claim 2, and is characterized by setting up said access restriction by the zoning function or masking function of said SAN.

[Claim 4] It is the backup management method of the data in storage in a storage system according to claim 2. Said encryption data is generated on real time according to change of the data stored in said hard disk unit A, and it is characterized by carrying out Storage and File Management Sub-Division of said encryption data to said hard disk unit other than said hard disk unit A in concurrency.

[Claim 5] The storage system equipped with a means to enforce the backup management method according to claim 1 to 4.

[Detailed Description of the Invention]

[0001]
[Field of the Invention] This invention relates to the technology for securing the data security at the time of carrying out backup management of the data in storage intensively especially using the backup unit of a removable media method about the backup management method of the data in storage in a storage system.
[0002]
[Description of the Prior Art] The demand of data centers is growing with expansion of an ASP market, and the outsourcing inclination of an enterprise system. The outline composition of the storage system in a typical data center is shown in drawing 6 . The storage 10, such as disk array equipment, and the server equipment 20a, 20b, and 20c which connects with the apparatus outside a data center through LAN, WAN, the Internet, etc., and intervenes between these and storage 10, The backup unit 30 (DAT tape drive) which backs up the data in storage 10 is connected by SAN (Storage Area Network)50.
[0003] By the way, in a data center, in order to employ scalable Merritt by package management of data in the maximum efficiently, it is common to make the data of a system which is different in one set of storage 10, or a different user intermingled, and to carry out operational administration. therefore, [ in a data center / storage resource /, such as a hard disk unit mounted in storage 10, / each ] usually Reservation of data security is aimed at by giving every system and access restriction for every user's computer using functions, such as zoning and masking.
[0004] On the other hand, the crisis management to troubles, such as a disk crush, is also important in a data center. Usually, in the data center, the backup unit 30 connected to SAN50 using the technique of the LAN free backup and the Saba Flea backup which employed the feature of SAN50 efficiently is performing intensive backup management. In addition, usually the operator for the thing of removable media methods, such as a comparatively inexpensive DAT tape drive of a bit unit price, being adopted in many cases, and desorbing a removable media to the backup unit 30 as the aforementioned backup unit 30, is stationed.
[0005]
[Problem to be solved by the invention] By the way, when desorbing the aforementioned removable media, careful cautions are required of an operator. because, when specified Media and different Media should be mistaken and it has set in the backup unit 30 It is because there is a possibility of the data of an alien system or a user being stored in the storage resource by which access restriction was carried out to a certain system and object for users, and leading to the serious accident in connection with trust of a data center.
[0006] However, since an operator is also man, it is difficult to prevent such an artificial mistake completely, therefore it is desirable on employment of a data center to establish the structure which prevents such an accident.
[0007] It aims at offering the storage system equipped with a means to enforce the backup management method of the data in storage in a storage system that this invention is made from such a viewpoint and high data security can be secured, and this management method.
[0008]
[Means for solving problem] [ main invention of this invention for attaining this purpose ] [ the server equipment which accesses the storage which has two or more storage areas to which access restriction was given individually, and this storage, and the backup unit of a removable media method / with predetermined means of communications ] It is the backup management method of the data in storage in the storage system by which network connection is carried out. [ with the key which gave the data of storage area A peculiar to storage area A ] on the occasion of backup of the data of certain storage area A of said storage areas The enciphered encryption data is stored in the predetermined removable media set in said backup unit through said communication network. The encryption data which sets the removable media of relevance in said backup unit when restoring the data of storage area A, and is stored in this is transmitted to said storage through said

communication network. It decrypts by said key to which this was given by storage area A, and is made to store in storage area A.
[0009]
[Mode for carrying out the invention] The outline composition of the storage system which is explained to drawing 1 as one working example of this invention and which was installed in the data center is shown. The disk array equipment 10 which functions as fiber channel storage, The server equipment 20 which connects with computers, such as a company which is the user of this data center, through external networks, such as LAN, and WAN or the Internet, and intervenes between these and disk array equipment 10, It connects with SAN50 which consisted of network devices, such as a fiber channel switch and a fiber channel bridge, and the DAT tape drive 30 constitutes the storage system.
[0010] Drawing 2 is the outline composition of disk array equipment 10. Various control and system-operating-status surveillance in the drive control section 12 which two or more sets of hard disk units 11 are mounted, and is these-controlled, the channel control section 13 which controls connection between SAN50, the shared memory 14 and cache memory 15, and disk array equipment 10, It has the service processor 16 which performs obstacle detection, variety-of-information management (for example, management of the physical number of cylinders of a hard disk unit 11, access frequency, etc. mounted), etc.
[0011] Access restriction is given to the hard disk unit 11 by functions with which a fiber channel switch, disk array equipment, etc. are equipped, such as zoning and masking. In the case of drawing 1 , for example, the hard disk units 11a and 11b, Although access restriction (zone a, b, and c) is individually given to 11c, respectively, and hard disk units 11a, 11b, and 11c constitute the storage area which became independent, respectively, for example, server equipment 20a can access the hard disk unit 11a of Zone a Neither the hard disk unit 11b of Zone b nor the hard disk unit 11c of Zone c can be accessed.
[0012] [ a part of hard disk unit 11 of disk array equipment 10 ] It is assigned to the unit A for acting before the audience in which direct read-out and the direct writing from server equipment 20a are possible, and other parts are assigned to the unit B for shunting for storing the backup data of the unit A for acting before the audience. [ matching with each unit A for acting before the audience, and the unit B for shunting ] It is set up by various kinds of methods, such as a way the method which a system administrator etc. sets up manually from the administration terminal of disk array equipment 10 etc., and a service processor 16 carry out automatic recognition of the position of a slot where each hard disk unit 11 is mounted, and set it up, for example. Disk array equipment 10 is carrying out Storage and File Management Sub-Division of the matching with this unit A for acting before the audience, and the unit B for shunting to the managed table shown in drawing 3 by the peculiar unit ID to which it was given by each hard disk unit 11.
[0013] The backup data stored in the unit B for shunting enciphers not the data of the unit A for acting before the audience itself but this. Disk array equipment 10 enciphers the data of each unit A for acting before the audience on real time, and stores it in the unit B for shunting matched with each unit A for acting before the audience on real time. Thereby, Storage and File Management Sub-Division of the data encryption data of the unit A for acting before the audience is carried out to the unit B for shunting in concurrency.
[0014] Encryption is performed using the key set up peculiar for every pair of each unit A for acting before the audience, and the unit B for shunting matched with this. A key is set up by various methods, when are automatically generated by disk array equipment 10, and manually set up by the system administrator etc. A key is matched with the combination of the unit A for acting before the audience, and the unit B for shunting, and Storage and File Management Sub-Division is carried out to said managed table.
[0015] by the way, [ the storage system explained in this working example ] On the occasion of backup of the data of the unit A for acting before the audience, he does not back up the data of the

unit A for acting before the audience as it is, but is trying to back up the encryption data stored in the unit B for shunting matched with this. This is for a series of processings about backup to reduce the influence on the various systems and user who stopped the load given to the unit A for acting before the audience as much as possible, and use the unit A for acting before the audience.
[0016] Backup is performed by the following procedure. First, disk array equipment 10 transmits set directions of a DAT tape to the DAT tape drive 30 through SAN50. Thereby, the DAT tape drive 30 displays that a DAT tape is set to an attached administrative display. The unit ID which specifies the unit A for acting before the audience used as the candidate for backup is contained, it attaches to an administrative display at said set directions, and Unit ID is displayed on these directions here. If these displays are checked, an operator will discover the DAT tape prepared for unit A for acting before the audience of relevance from a managed rack, and will set to the DAT tape drive 30.
[0017] Next, if a DAT tape is set normally, that will be notified to disk array equipment 10 through SAN50. The encryption data stored in the unit B for shunting corresponding to the unit A for acting before the audience used as the candidate for backup leads SAN50, it is transmitted to the DAT tape drive 30 from disk array equipment 10, and said encryption data is stored in said DAT tape. Completion of storing on the DAT tape of encryption data will display that on an administrative display. The operator who looked at this removes a DAT tape from the DAT tape drive 30, and stores the DAT tape in the predetermined position of an administrative rack.
[0018] On the other hand, the encryption data backed up by the DAT tape is used for restoration processing of data when the data of the unit A for acting before the audience carries out loss etc. by a disk crush etc., for example. Below, the procedure of this restoration processing is explained with the flow chart shown in drawing 4 .
[0019] If it judges that the encryption data which a certain abnormalities occurred to a certain unit A for acting before the audience, and was backed up by the DAT tape needs to be used for disk array equipment 10 Set directions of the DAT tape on which the encryption data (namely, encryption data which backed up from the unit B for shunting corresponding to this unit A for acting before the audience) corresponding to that unit A for acting before the audience is stored in the DAT tape drive 30 are transmitted through SAN50 (110). The DAT tape drive 30 will display the unit ID of said unit A for acting before the audience accompanying this that and set request notice on an administrative display, if these set directions are received (120). If these set directions are checked, an operator will discover the DAT tape of relevance from a managed rack, and will set that tape to a DAT tape drive (130).
[0020] If a DAT tape is set normally, next, that will be notified to disk array equipment 10 through SAN50, and the encryption data stored in the DAT tape set to the DAT tape drive 30 will be transmitted to disk array equipment 10. Disk array equipment 10 stores the transmitted encryption data in the unit B for shunting matched with said unit A for acting before the audience (140).
[0021] If encryption data is stored in the unit B for shunting by the above, disk array equipment 10 will try next a decoding of the encryption data memorized by the unit B for shunting by the key matched with said unit A for acting before the audience with reference to a managed table (150). When this key is in agreement with the key used on the occasion of the encryption data encryption stored in the unit B for shunting here A decoding is performed normally, disk array equipment 10 stores the decrypted data in said unit A for acting before the audience, and, thereby, data restoration processing of said unit A for acting before the audience completes it safely (160).
[0022] On the other hand, when a key is inharmonious, it cannot decrypt but disk array equipment 10 displays the error message which notifies that to the display of the administration terminal of the equipment 10 concerned etc. in this case (170). [ and the system administrator who got to know what a decoding was not able to carry out seeing this ] it checks [ of a DAT tape ] to an operator whether the mistake has been made in whether hanging or not, and when a mistake is made in hanging, it comes out and it is, correspondence of rehaving the right DAT tape set to the DAT tape drive 30 will be devised to an operator.

[0023] [ according to this invention ] even if an operator makes a mistake in hanging a DAT tape and sets it as explained above If a key is not in agreement at all even if the encryption data of an alien system or a user is stored in the hard disk unit by which access was permitted to a certain system and user, the encryption data will not be decrypted and high data security will be secured. Moreover, if a key should not be known at all even if a DAT tape is stolen, the original data cannot be restored but data security will be secured also at this point.
[0024] By the way, [ the working example ] although the above working example was the composition of backing up the encryption data stored in the unit B for shunting For example, disk array equipment 10 enciphers the data of the unit A for acting before the audience directly. Transmit this encryption data to the DAT tape drive 30 through direct SAN50, and it backs up to a removable media. The composition of transmitting to disk array equipment 10 and decrypting through [ SAN50 ] the encryption data stored in the DAT tape of relevance at the time of data restoration from a DAT tape drive is also considered. In addition, when this method is adopted, as shown in drawing 1 , two or more hard disk units do not necessarily need to be contained in each zone, and one set only of a hard disk unit needs to be contained in one zone.
[0025] The method of access restriction of it not being necessarily necessary to set up access restriction per hard disk unit for example, as the above-mentioned working example explained, and it dividing the storage area of one set of a hard disk unit, and giving a divided different access restriction for every storage area is also considered.
[0026] The unit A for acting before the audience and the unit B for shunting may be matched with 1:1 like the above-mentioned working example, and may be matched with 1:n.
[0027] Storage may not be restricted when it is disk array equipment, but a magnetic disc system, optical-magnetic disc equipment (what was both equipped with the cache and buffer of sufficient capacity), etc. are sufficient as it.
[0028] [ a backup unit ] in addition to the DAT tape drive mentioned above For example, a cassette tape, a 8mm tape, 9 truck opening tape, 3490 / 3490E cartridge, a DLT/SDLT tape, You may use Media, such as an AIT tape, a TRAVAN minicartridge tape, a DTF cartridge, a LTO cartridge, ZIP, CD-R, DVD-RAM, DVD-R, MO, and a floppy (registered trademark) disk.
[0029] Moreover, although the hard disk unit 11 generally mounted in storage constitutes RAID in many cases, it can concern for it and apply this invention to whether RAID is constituted or not.
[0030] A key may assign the same key to the both sides of encryption and a decoding like the above-mentioned working example, and may set up a cryptographic key and a decoding key separately. In addition, a cryptographic key and a decoding key will be managed by the managed table with a form as shown in drawing 5 in this case, for example.
[0031] Moreover, although premised on a secret key method in the above explanation, adopting a public-key-encryption-ized method is also considered.
[0032]
[Effect of the Invention] As explained above, according to this invention, it is possible to perform backup management of the data in storage in a storage system, securing high data security.

---

[Brief Description of the Drawings]
[Drawing 1] It is the figure showing the outline composition of the storage system installed in the data center by one working example of this invention.
[Drawing 2] It is the figure showing the outline composition of the disk array equipment by one working example of this invention.
[Drawing 3] It is the figure showing an example of the managed table by one working example of this invention.
[Drawing 4] It is a flow chart explaining restoration processing of the data of the unit for acting

before the audience by one working example of this invention.
[Drawing 5] It is the figure showing an example of the managed table by one working example of this invention.
[Drawing 6] It is the figure showing the outline composition of the storage system in the conventional data center.
[Explanations of letters or numerals]
10 Disk Array Equipment
11 Hard Disk Unit
20a, 20b, 20c Server equipment
30 Backup Unit (DAT Tape Drive)
50 SAN

---

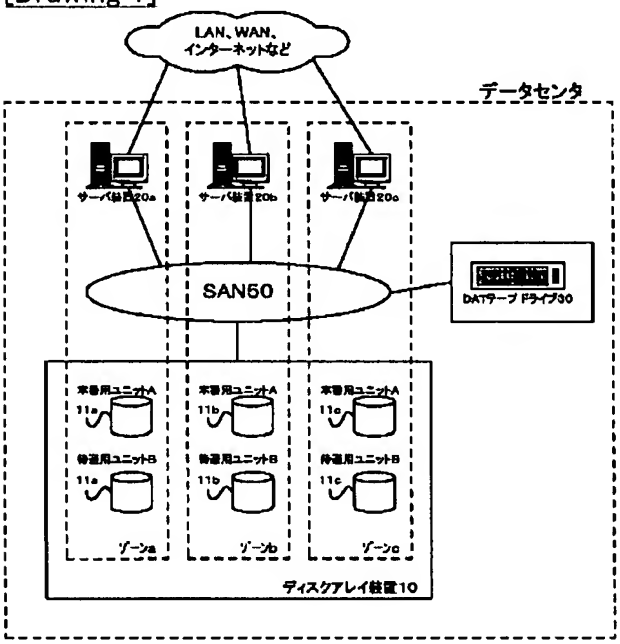
[Drawing 3]

| 本番用ディスクのユニットID | 待避用ディスクのユニットID | 暗号化キー |
|---|---|---|
| 500 | 600 | xxxyyyzzz |
| 114 | 116 | xxxzzzyyy |
| 118 | 120 | wwwssskkk |
| . | . | . |
| . | . | . |
| . | . | . |
| . | . | . |
| . | . | . |

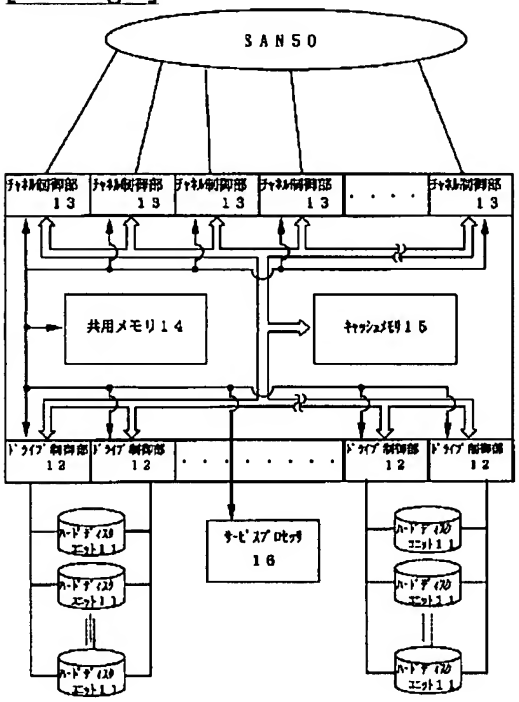
[Drawing 5]

| 本番用ディスクのユニットID | 待避用ディスクのユニットID | 暗号化キー | 復号化キー |
|---|---|---|---|
| 500 | 600 | xxxyyyzzz | ssskkkjjj |
| 114 | 116 | xxxzzzyyy | pppqqquuu |
| 118 | 120 | wwwssskkk | yyyrrrlll |
| . | . | . | . |
| . | . | . | . |
| . | . | . | . |
| . | . | . | . |
| . | . | . | . |

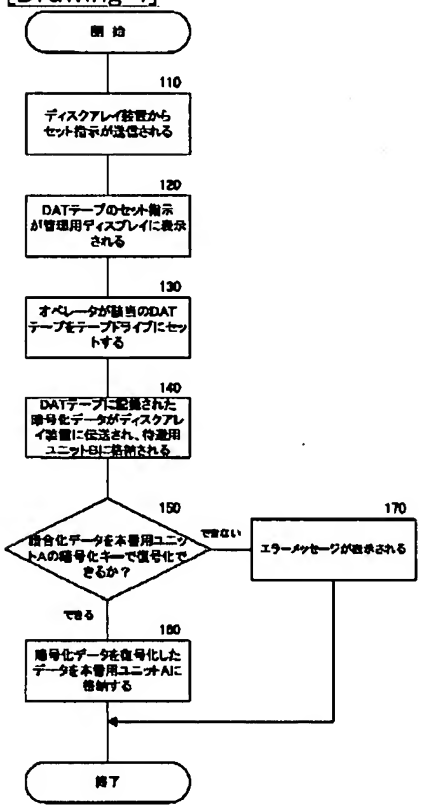
[Drawing 1]



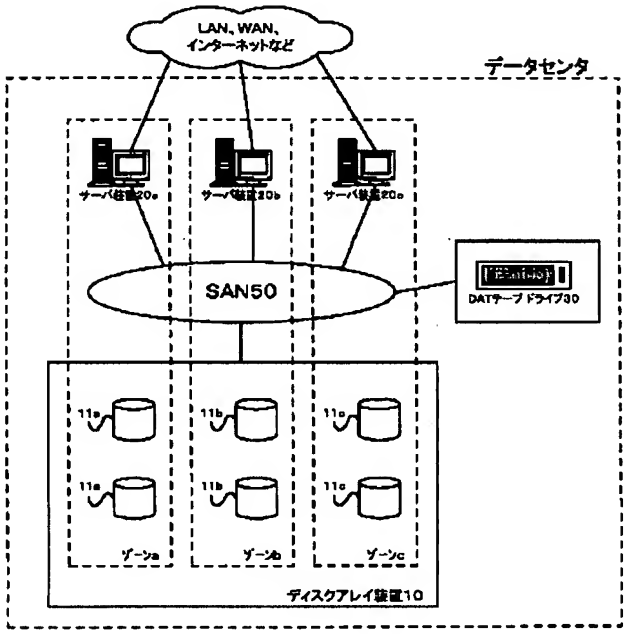
[Drawing 2]




[Drawing 4]




[Drawing 6]




---

[Translation done.]